

AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions of claims in the application:

Listing of Claims:

1. (Currently Amended) A security analysis tool for an automation system, comprising:
an interface component ~~to generate~~ that generates a description of one or more industrial controllers, wherein the description includes at least one of shop floor access patterns, Intranet access patterns, Internet access patterns, and wireless access patterns; ~~and~~
an analyzer component ~~to generate~~ that generates one or more security outputs based on the description; and
a validation component that periodically monitors the industrial network controllers following deployment of the one or more security outputs to determine one or more vulnerabilities related thereto.
2. (Original) The tool of claim 1, at least one of the interface component and the analyzer component operate on a computer and receive one or more factory inputs that provide the description.
3. (Original) The tool of claim 2, the factory inputs include user input, model inputs, schemas, formulas, equations, files, maps, and codes.
4. (Original) The tool of claim 2, the factory inputs are processed by the analyzer component to generate the security outputs, the security outputs including at least one of manuals, documents, schemas, executables, codes, files, e-mails, recommendations, topologies, configurations, application procedures, parameters, policies, rules, user procedures, and user practices that are employed to facilitate security measures in an automation system.

5. (Original) The tool of claim 1, the interface component includes at least one of a display output having associated display objects and at least one input to facilitate operations with the analyzer component, the interface component is associated with at least one of an engine, an application, an editor tool, a web browser, and a web service.

6. (Original) The tool of claim 5, the display objects include at least one of configurable icons, buttons, sliders, input boxes, selection options, menus, and tabs, the display objects having multiple configurable dimensions, shapes, colors, text, data and sounds to facilitate operations with the analyzer component.

7. (Original) The tool of claim 5, the at least one inputs includes receiving user commands from a mouse, keyboard, speech input, web site, remote web service, camera, and video input to affect operations of the interface component and the analyzer component.

8. (Original) The tool of claim 1, the description includes a model of one or more industrial automation assets to be protected and associated network pathways to access the industrial automation assets.

9. (Original) The tool of claim 1, the description includes at least one of risk data and cost data that is employed by the analyzer component to determine suitable security measures.

10-11. (Cancelled).

12. (Currently Amended) A security analysis method, comprising:
inputting at least one model related to one or more industrial controllers;
monitoring access to the industrial controllers to learn at least one access pattern; ~~and~~
generating one or more security outputs based on the model; and
performing one or more automated actions based at least in part on detecting a deviation from the at least one learned access pattern.

13. (Original) The method of claim 12, the at least one model is related to at least one of a risk-based model and a cost-based model.
14. (Original) The method of claim 12, the security outputs include at least one of recommended security components, codes, parameters, settings, related interconnection topologies, connection configurations, application procedures, security policies, rules, user procedures, and user practices.
15. (Original) The method of claim 12, further comprising at least one of:
automatically deploying the security outputs to one or more entities; and
utilizing the security outputs to mitigate at least one of unwanted network access and network attack.
16. (Currently Amended) A security analysis system in an industrial automation environment, comprising:
means for receiving abstract descriptions of one or more industrial controllers;
means for learning at least one access pattern for accessing the industrial controllers;
means for generating one or more security outputs based on the abstract description; ~~and~~
means for automatically distributing the security outputs to facilitate network security in the industrial automation environment;
means for detecting a deviation from the at least one access pattern; and
means for performing an automated action based at least in part on the detected deviation.
17. (Currently Amended) A security validation system, comprising:
a scanner component to automatically interrogate an industrial automation device at periodic intervals for security related data; ~~and~~
a validation component to automatically assess security capabilities of the industrial automation device based upon a comparison of the security related data and one or more predetermined security guidelines; and
a security analysis tool that recommends interconnection of one or more industrial automation devices to achieve a specified security goal.

18. (Cancelled).
19. (Original) The system of claim 17, the validation component performs at least one of a security audit, a vulnerability scan, a revision check, an improper configuration check, file system check, a registry check, a database permissions check, a user privileges check, a password check, and an account policy check.
20. (Original) The system of claim 17, the security guidelines are automatically determined.
21. (Original) The system of claim 46, the host-based component performs vulnerability scanning and auditing on devices, the network-based component performs vulnerability scanning and auditing on networks.
22. (Cancelled).
23. (Previously Presented) The system of claim 21, at least one of host-based component and the network-based component at least one of includes non-destructively mapping a topology of IT and industrial automation devices, checking revisions and configurations, checking user attributes, and checking access control lists.
24. (Currently Amended) The system of claim 17, further comprising a component to automatically ~~initiate a security action~~ install one or more security components in response to detected security problems.
25. (Original) The system of claim 24, the security action includes at least one of automatically correcting security problems, automatically adjusting security parameters, altering network traffic patterns, add security components, removing security components, firing alarms, automatically notifying entities about detected problems and concerns, generating an error or log file, generating a schema, generating data to re-configure or re-route network connections, updating a database, and updating a remote site.

26. (Currently Amended) An automated security validation method, comprising:
scanning one or more industrial automation devices for potential security violations at periodic intervals, wherein identity information about end devices that relates to hacker entry is gained;~~and~~
performing an automated security procedure ~~if a security violation is detected~~ on the one or more industrial automation devices based at least in part on the potential security violations;
and
determining whether the industrial automation device conforms to one or more industry standards following performing the automated security procedure thereon.
27. (Original) The method of claim 26, further comprising at least one of:
checking for susceptibility to network-based attacks;
searching for open TCP/UDP ports; and
scanning for vulnerable network services.
28. (Original) The method of claim 26, further comprising at least one of:
automatically performing security assessments;
automatically performing security compliance checks; and
automatically performing security vulnerability scanning.
29. (Original) The method of claim 26, the automated security procedures include at least one of automatically performing corrective actions, altering network patterns, adding security components, removing security components, adjusting security parameters, and generating security data to mitigate network security problems.

30. (Currently Amended) An automated security validation system, comprising:
means for scanning one or more industrial automation devices for potential security violations;
means for initiating a security procedure in response to the security violations; and
means for performing at least one of security assessments, security compliance checks, and security vulnerability scanning of the industrial automation devices to mitigate the security violations based at least in part on the initiated security procedure.
31. (Original) A security learning system for an industrial automation environment, comprising:
a learning component to monitor and learn industrial automation activities during a training period; and
a detection component to automatically trigger a security event based upon detected deviations of subsequent industrial automation activities after the training period.
32. (Previously Presented) The system of claim 31, the industrial automation activities includes at least one of a network activity and a device activity.
33. (Original) The system of claim 31, the learning component including at least one of a learning model and a variable
34. (Original) The system of claim 31, the industrial automation activities include at least one of a number of network requests, a type of network requests, a time of requests, a location of requests, status information, and counter data.
35. (Original) The system of claim 31, the detection component employs at least one of a threshold and a range to determine the deviations.
36. (Original) The system of claim 35, the threshold and the range are dynamically adjustable.

37. (Original) The system of claim 33, the learning model includes at least one of mathematical models, statistical models, probabilistic models, functions, algorithms, and neural networks, classifiers, inference models, Hidden Markov Models (HMM), Bayesian models, Support Vector Machines (SVM), vector-based models, and decision trees.

38. (Original) The system of claim 31, the security event includes at least one of automatically performing corrective actions, altering network patterns, adding security components, removing security components, adjusting security parameters, firing an alarm, notifying an entity, generating an e-mail, interacting with a web site, and generating security data to mitigate network security problems.

39. (Currently Amended) A security learning method, comprising:
monitoring a network of industrial controllers for a predetermined time;
automatically learning at least one data pattern of the network of industrial controllers during the predetermined time; and
generating an alarm ~~if~~ where a current data pattern is determined to be outside of a predetermined threshold associated with the at least one data pattern.

40. (Original) The method of claim 39, the at least one data pattern employed as input for a security analysis process.

41. (Currently Amended) A security learning system in an automation environment, comprising:
means for scanning a network;
means for learning access patterns to at least one industrial automation device from the network; and
means for generating a security event ~~if~~ where the current access patterns are determined to be out of tolerance from stored access patterns.

42-44. (Cancelled).

45. (Previously Presented) The tool of claim 1, the analyzer component is adapted for partitioned security specification entry and sign-off from various groups.

46. (Previously Presented) The system of claim 17, the scanner component and the validation component are at least one of a host-based component and a network-based component.

47. (Previously Presented) The system of claim 21, at least one of host-based component and the network-based component at least one of determines susceptibility to common network-based attacks, searches for open TCP/UDP ports, scans for vulnerable network services, attempts to gain identity information about end devices that relates to hacker entry, performs vulnerability scanning and auditing on firewalls, routers, security devices, and factory protocols.